NASA Policy Directive

NPD 1382.17J
Effective Date: June 29, 2016
Expiration Date: November 30, 2021

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Privacy Policy

Responsible Office: Office of the Chief Information Officer

1. POLICY

a. NASA's policy is to protect all forms of sensitive unclassified information, including personal information.

b. Federal law and regulations require that all personal information collected, used, maintained, and disseminated by or on behalf of this Agency is included whether in electronic or non-electronic form.

c. Therefore, NASA policy requires that:

(1) All collections of sensitive unclassified information (including personal information as defined in Attachment A of this NPD) will be assessed for applicability under, managed, and appropriately protected in compliance with Federal laws, regulations, and Government-wide policies.

(2) An Initial Privacy Threshold Analysis (IPTA) for any new, or significantly changed, applications, Web sites, information systems (including third party applications and information systems and collections of information provided for by external service providers who are collecting information on behalf of NASA), and all non-electronic information collections will be accomplished to determine whether there are any privacy implications or other regulatory compliance requirements.

(3) When initial assessments via the IPTA process calls for the completion of a full Privacy Impact Assessment (PIA), one will automatically be initiated and must be completed prior to actively collecting any information. (4) All collections of personal information gathered by or on behalf of NASA will leverage Agency-specific individual identifiers. The use of Social Security Numbers (SSNs) will be avoided to the greatest extent possible. In instances where SSNs are already in use, collections will be reviewed annually for removal or replacement using other Agency individual identifiers (such as the Universal Uniform Personal Identification Code (UUPIC). The use of SSNs is authorized only when mandated by external or statutory requirements and justified in writing within the associated IPTA or PIA.

2. APPLICABILITY

a. This NASA Policy Directive (NPD) is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to all contractors providing services to NASA, including the Jet Propulsion Laboratory, a Federally Funded Research and Development Center, grant recipients, or parties to agreements to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. This NPD is applicable to all NASA users (e.g., civil servants and contractors) when collecting personal information in support of Agency projects, programs, and missions.

c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is

recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

3. AUTHORITY

a. National Aeronautics and Space Act, as amended, 51 United States Code (U.S.C.) § 20101 et seq.

b. Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

c. Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 et seq.

d. E-Government (e-Gov) Act of 2002, as amended, 44 U.S.C. § 3601 et seq.

e. Paperwork Reduction Act of 1995 (PRA), 44 U.S.C. § 3501 et seq., as amended.

f. Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § 6501 et seq., 16 C.F.R part 312.

4. APPLICABLE DOCUMENT AND FORMS

a. NASA Privacy Act Regulations, 14 CFR Part 1212.

b. NPD 2810.1E, NASA Information Security Policy.

c. OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites.

d. OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.

e. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

f. OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy.

g. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information.

h. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost of Security in Agency Information Technology Investments.

i. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).

j. National Institute of Standards and Technology (NIST) Special Publications.

5. RESPONSIBILITY

a. NASA Administrator shall:

(1) Designate the NASA Chief Information Officer (CIO) as the NASA Senior Agency Official for Privacy (SAOP).

(2) Delegate to the SAOP the overall responsibility and accountability for ensuring NASA's implementation of personal information protections, including the Agency's full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

b. SAOP shall:

(1) Have the primary responsibility for the development and implementation of the Agency's privacy policy.

(2) Carry out the NASA Administrator's responsibilities for privacy.

(3) Review and approve PIAs.

(4) Provide OMB with PIAs for planned Information Technology (IT) systems and for collections of information from the public as required.

(5) Appoint the NASA Chief Privacy Officer (CPO),(a role synonymous with and also referred to as Privacy Program Manager (PPM)).

(6) Delegate to the NASA CPO oversight, governance, training, and implementation responsibilities for privacy activities.

(7) Appoint the NASA Privacy Act Officer (PAO).

(8) Establish and chair a Data Integrity Board to oversee and coordinate among the various components of the Agency if and when NASA conducts or participates in a matching program in accordance with the requirements of the Privacy Act of 1974.

c. NASA's CPO shall:

(1) Respond to actions issued by Congress or external Agencies, oversee, manage, and implement the Federal Privacy laws, regulations, and NASA and Government-wide policies as directed by the SAOP.

(2) Ensure compliance with privacy provisions contained in Federal statutes, including the collection, maintenance, use, and dissemination of personal information.

(3) Develop and maintain NASA privacy policies, procedural requirements, handbooks, and memoranda.

(4) Establish Agency requirements and processes for conducting IPTAs and PIAs for new or significantly changed applications, Web sites, or information systems, and make PIAs publicly available (unless public release is otherwise prohibited).

(5) Develop and submit Agency privacy reports required by OMB and FISMA.

(6) Provide final quality reviews for all Agency PIAs, System of Records Notice (SORNs), communications, and other documents routed to the SAOP for approval prior to issuance or publication in the Federal Register.

(7) Develop and manage required privacy training and outreach to meet Federal requirements and maintain a state of heightened awareness regarding the protection of NASA personal information.

d. NASA Privacy Act Officer shall:

(1) Provide overall management and oversight to ensure compliance with Privacy Act requirements.

(2) Ensure inclusion of Privacy Act requirements in NASA policy.

(3) Conduct regular Privacy Act review and reporting activities as required by the Privacy Act and OMB directives.

(4) Maintain effective communication with Center Privacy Managers and other NASA personnel with respect to meeting Privacy Act requirements.

e. Center Directors and the Director of Headquarters Operations shall:

(1) Ensure Center compliance with NASA privacy policies and requirements.

(2) Designate a Center Privacy Manager (CPM).

f. Center CIOs shall:

(1) Ensure Center implementation of and adherence to NASA privacy policy and requirements through the respective CPM.

(2) Ensure that Information Owners (IOs) and Information System Owners (ISOs) assess the privacy aspects of information collections and information systems for which they are responsible, and ensure all required security safeguards are implemented in accordance with current NASA policy and procedural requirements for the collection, use, maintenance, and dissemination of personal information.

(3) Ensure the CPM is engaged and directly involved with all privacy related information compromises and incidents, whether potential or confirmed.

g. CPM shall:

(1) Serve as the Center's foremost expert and consultant on all Center related NASA privacy matters, including overseeing, managing, and implementing NASA privacy policies and procedural requirements for their respective Center.

(2) Serve as the interface between the NASA CPO and Center personnel on privacy matters.

(3) Provide the Center's privacy reports as required by the NASA CPO in support of OMB, FISMA, and Agency requirements.

(4) Ensure that IOs and ISOs perform the required information collection assessments (IPTAs and PIAs as required) and aid in the development of any additional documentation indicated as required upon completion of the IPTA (or PIA if required). (This includes SORNs, Privacy Act Federal Register notices, and Privacy Act Statements.)

(5) Lead at the Center level all Agency-wide privacy reviews and actions as requested by the NASA CPO or PAO.

(6) Participate in and provide oversight, guidance, and support for all Center-related and Agency-wide (as applicable) Privacy Breach Response Team (BRT) activities, investigations, and reporting of PII potential or confirmed breach incidents. Notify and regularly update the NASA CPO throughout the BRT process.

(7) Conduct a local, or support Agency annual Privacy BRT exercise each fiscal year in accordance with NASA procedural requirements, and report completion and lessons learned to the NASA CPO.

h. Heads of Mission Directorates and Mission Support Offices (MSOs) may appoint a Mission Privacy Point of Contact (MPPOC), with the same relative privacy accountability as that of the CPMs as outlined in this and other Agency privacy directives, with direct accountability to act as a liaison in providing the necessary support to the CPM for Center-wide privacy related reporting and operational activities.

(1) If a Mission Directorate or MSO PPOC is not appointed, the CPM shall fulfill the privacy responsibilities for the Mission Directorate and MSO activities located at, or under the cognizance of, the related Center.

i. Information Owners (IOs) and Information System Owners (ISOs) shall:

(1) Ensure all personal information collected under their purview is properly identified and assessed via the IPTA or PIA as appropriate, during the earliest possible milestones of, and at each key decision point throughout the life-cycle management process, to validate the information is appropriately protected, managed, and controlled, prior to any active collection of, or creation of new collections.

(2) Ensure the secure transmission and storage of personal information collected by their system(s) in accordance with Federal law, regulations, Government-wide and NASA policy and procedural requirements.

(3) Conduct and fully support annual privacy review and reduce activities for collections of PII and SSNs, as well as other Agency-level reporting requirements and data call actions as relayed via CPMs in support of annual FISMA and other Federal or Agency requirements.

j. All NASA Users (civil servant and contractor) shall:

(1) Protect all personal information (whether electronic or non-electronic) for which they are responsible or that is in their custody, in accordance with this and other NASA policies, procedures, handbooks, and memoranda.

(2) Ensure any electronic storage or dissemination of personal information is encrypted when in electronic transmission or at rest (including extracts), in addition to data at rest (DAR) encryption.

(3) Ensure that any personal information in their custody is disseminated only to those individuals who have the official need to know the information in the performance of their duties.

(4) Immediately report any PII potential or confirmed breaches (e.g., loss, inappropriate access, or unauthorized disclosure) immediately upon discovery, directly to the NASA Security Operations Center (SOC).

(5) Participate in required privacy training upon reporting to NASA and annually thereafter, to ensure and maintain heightened awareness of their privacy responsibilities.

6. DELEGATION OF AUTHORITY

The NASA SAOP is delegated authority to carry out the functions and exercise the authority vested in the Administrator to implement, oversee, and manage privacy policy within the Agency pursuant to the authorities cited above.

7. MEASUREMENT/VERIFICATION

a. The effectiveness of this directive will be assessed as follows:

(1) Measurements should be collected and evaluated by the NASA SAOP to assess the effectiveness of this policy directive at least annually by measuring the degree of compliance with the NIST privacy controls, including that PIAs are documented, continue to adequately represent the collection, that the privacy and security controls outlined therein continue to be in place, and that the PIAs are made publicly available (if permitted).

(2) Measurements should be collected and evaluated by the NASA SAOP at least annually to assess trends involving PII incidents and trends for tracking metrics involving the cost and effect on mission, program, and project performance attributed to the loss or unauthorized access to personal information.

(3) The NASA SAOP will publish revised Federal Register Privacy Act notices, as required through biennial review.

(4) The NASA SAOP will evaluate the Agency's Privacy Program and provide the Agency's SAOP FISMA response to OMB.

8. CANCELLATION

NPD 1382.17H, NASA Privacy Policy, dated June 24, 2009.

/s/ Charles F. Bolden
Administrator

ATTACHMENT A: (TEXT)

Data Extracts are created when information from a pre-existing data source is exported, thereby creating a new and separate information collection.

Information in identifiable form (IIF), in accordance with section 208(d) of the e-Gov act, IIF is defined as "... any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

In accordance with OMB Memorandum M-03-22, IIF "... is information in an IT system or online collection: (i) that directly identifies an individual (e.g. name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."

NASA User is any explicitly authorized patron of a NASA information system. The NASA user includes, but is not limited to, civil servants and contractors.

Personally identifiable information, in accordance with M-07-16, PII "... refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

In accordance with M-10-23, "... [t]he definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual."

For purposes of NASA policy, sensitive PII excludes personal information collected and or maintained by NASA employees and contractors for personal rather than NASA business purposes, as allowed under NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

Examples of such excluded data include contact information for family, relatives, and doctors.

NASA defines PII commensurate with OMB Memoranda M-07-16 and M-10-23 with further definition as it applies to sensitive and non-sensitive PII. Sensitive PII is well defined above however, Non-Sensitive PII though it is PII, is information that is available through commonly available public sources, the disclosure of which cannot reasonably be expected to result in personal harm or embarrassment.

For the purposes of this policy as it applies to IPTAs and PIAs, significant change is defined as any change that constitutes new uses of existing information being collected, application of new technologies (such as non-electronic collection to electronic, implementation of persistent tracking technology (cookies), how information is collected or managed, from whom the information is to be collected, duration of information retention, how the information is being collected (e.g., forms, electronic or non-electronic), or any change to the application, system, Web site, Web application or information collection (including change in NASA responsible official, information owner or system owner), that effects how the information is stored, managed, and protected.

Privacy Act Information is any information which is subject to the requirements established by the Privacy Act of 1974 and NASA Privacy Act Regulations, 14 Code of Federal Regulations (CFR) Part 1212 - The Privacy Act sets forth extensive requirements for the management of personal information contained in a system of records (SOR),

where such information is routinely retrieved by a name or personal identifier unique to the individual.

Privacy Information (or personal information), is any information, which falls within the definitions of IIF, PII, or Privacy Act as described herein.

Laws, regulations, and guidance documents provide various terms and definitions used to describe personal or personal information. These include: personally identifiable information or PII, personal information, Privacy Act records, and IIF.

ATTACHMENT B: ACRONYMS

CIO Chief Information Officer

CISO [Center] Chief Information Security Officer

COPPA Children's Online Privacy Protection Act

CPM Center Privacy Manager

CPO Chief Privacy Officer (Synonymous with Privacy Program Manager (PPM)) e.g. exempli gratia (for example)

FISMA Federal Information Security Management Act

IIF Information in Identifiable Form

IO Information Owner

IPTA Initial Privacy Threshold Analysis (Sometimes referred to as

Information Privacy Threshold Analysis, or Initial Information Privacy Threshold Analysis)

ISO Information System Owner

JPL Jet Propulsion Laboratory (a FFRDC)

NASA National Aeronautics and Space Administration

MPPOC Mission Directorate and Mission Support Offices (MSOs) Appointed

Privacy Point of Contact

MSO Mission Support Office

NIST National Institute of Standards and Technology

NITR NASA Information Technology Requirement

NPD NASA Policy Directive

NPR NASA Procedural Requirement

OCIO Office of the Chief Information Officer

OMB Office of Management and Budget

PIA Privacy Impact Assessment

PII Personally Identifiable Information

PRA Paperwork Reduction Act

PPM Privacy Program Manager (Synonymous with Chief Privacy Officer (CPO))

SAISO Senior Agency Information Security Officer

SAOP Senior Agency Official for Privacy

SOC Security Operations Center

SORN Privacy Act of 1974 System of Records Notice

SSN Social Security Number

U.S.C. United States Code

UUPIC Universal Uniform Personal Identification Code or UUPIC is a number NASA uses in place of a social security number.

ATTACHMENT C: REFERENCES

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications.

NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

NID 1600.55, Sensitive But Unclassified Information.

(URL for Graphic)

None.

DISTRIBUTION:
NODIS

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.